SAP Community

Ask a Question Write a Blog Post Login

Alessandro Banzer

August 21, 2014 | 7 minute read

Remediating Access Control SoD Risks

26 18 21,767

Follow

Like

RSS Feed

GRC's Access Risk Analysis is a tool within Access Controls to enable you to define user access risk (via way of a rule set); execute risk analysis to identify access risk (or simulate for potential risk); and then provide you with system functionality to remediate the risk or mitigate via assignment of a control. As this is an approach, it can apply to any version of GRC (of course the system screen shots are in 10.x version).

Like any other risk process the reviewer is has four options: accept; transfer; mitigate or remediate. This document details our strategy and approach to risk remediation. Our position is that you should always attempt to remediate a risk before your mitigate. Remediation removes the risk (or the residual level is acceptable) from the system and does not rely on the use of compensating control (typically manual control that requires a person to take regular action and can be subjected to human error). Accepting and transferring of risk are last resorts. Of-course the your decision would involve a cost-benefit analysis. It makes not sense to spend more on the control than the true cost of the risk (financial, reputation, legal and compliance, etc).

When a risk has been identified (violation, issue, etc.) someone has to take action to resolve it. Depending on your master data setup, GRC automatically displays the risk definition, including who is responsible (risk owner); the respective business process; as well as mitigation owners/monitors. This information is important to enable your to know who to contact to discuss the risk and receive advise (and some of this interaction will occur off system).

Risk Violation Count is Massive (Why?)

Be aware that the first time you run a risk analysis it is likely that the number of violations will be very high. Users may have access creep due to change in job function and retained old access. Roles may have been built with too much access. At the time, the business did not have adequate tools to identify these risks. Many organisations undergo a security redesign project once they have implemented GRC due to the number of inherent conflicts in their roles. In the end they find it easier to completely rebuild security (get it right and clean first time) than try to unpick the issues and clean the existing roles. In some cases, companies are aware of the issues but mistakenly believe implementing GRC will fix it: all GRC will do is give you the number of violations and will not help you if you do not go down the path of remediation and mitigation.

For example, in the screen shot below there are over 200,000 conflicts (more if we scrolled down). This number is large – huge – and probably daunting when it comes to fixing it. After all where would you start? Remember a risk violation is one rule in the risk definition being met. Therefore, if a risk has two functions and both functions have two actions you then have 4 rule violations. If a user happens to have all four actions they too have 4 violations. If there are 50 derived roles, you will see the violation count increase to 200 (4 x 200). In the screen shot below, on further analysis (not visible in this screen shot) the bulk of the issues are caused by derived roles. By cleaning the imparting roles the number of violations will reduce substantially (also, you cannot clean a derived role without using PFCG incorrectly or actually fixing the imparting role).

Result

View: * [Standard View] | Display As: Table | Export | Type: Permission Level | Format: Executive Summary | Filter Settings

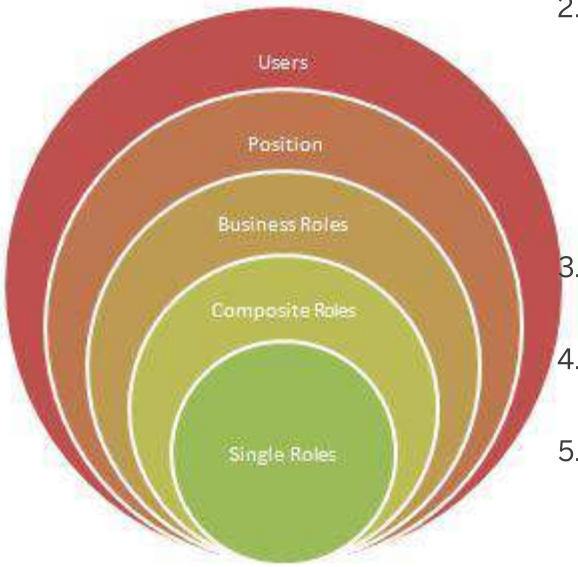
Access Risk ID	No. of Conflict	No. of Mitigation	SOD Object
XGPR0002	56,961		
XGPR0008	51,035		
XGHR0001	35,731		
XGSD0002	26,601		
XGPR0017	23,747		
XGFI0003	21,157		
XGPR0010	17,002		
XGPR0009	10,075		
XGPR0007	9,890		
XGPR0001	9,431		

Where to start for Remediation (Still overwhelmed by so many violations)?

Your security role design as well as access provisioning strategies will impact how you approach remediation. This diagram below assumed position-based security is used in your organisation. Depending on the authorisation concept and access management in your system, the number of circles will vary. For example, you may not user business roles or composite roles.

When approaching risk remediation, use the diagram below as a reference and work your way from the inside out.

1. ***Single Roles:*** focus on remediating conflict in your imparting roles and other non-derived single roles. You will fix the derived roles when you distribute the change from the imparting (assuming you have followed SAP standard security rules and not added additional authorisations to your derived). Single role clean up will involved removal of transactions and other authorisations.



2. ***Composite Roles:*** by this stage you expect that none of the single roles have inherent conflict. You cannot remediate risk in a composite role if the single role has conflict. Your choice to remediate at this point is to remove roles assigned to the composite (possible replace with a different version). Another option is to remove access from the single (it may not cause an inherent conflict in the single) if the access is not required and it is contributing to the violation.
3. ***Business Roles:*** this assumes you have built business roles via GRC Business Role Management for provisioning. Same principal applies as composite.
4. ***Positions:*** if you are using position based security then you can consider removing roles (single, derived, composite, etc) from the position.
5. ***Users:*** finally you have removed all inherited risk. The only unmitigated risk violations against the user is due to the combination of access. At this stage you can then remove roles.

Note: Remediating inherent role conflict will take time. You will need to work with the business process owners (the business) to determine the appropriate solution. Once you identify the permissions to removal from a role you will then need to follow your companies change management process to schedule the change and arrange a transport to Production. As an interim measure, you may need to implement a mitigating control.

Who should I engage with? What should I say?

This will depend on your company's organisational model and approach to risk management. However, regardless of approach it is still a business decision. You will need to consider meeting with the business process owners, line managers, etc.

In starting the conversation with these stakeholders you need to outline and explain what the risk is and why it needs to be remediated. In some cases the conversation may be as simple as 'Is this access really required'. You may discover over time that access creep has cause the conflict and requires clean-up. Where a user is concerned, the question may be 'Does this user really need both access'. The stakeholders identify non-compliance in a job duties or that there is an alternative person to take on part of the function. Again, it will all depend on the business so get out there and talk to the stakeholders!

For some more ideas refer to Reviewing of Risks in the: Risk Lifecycle

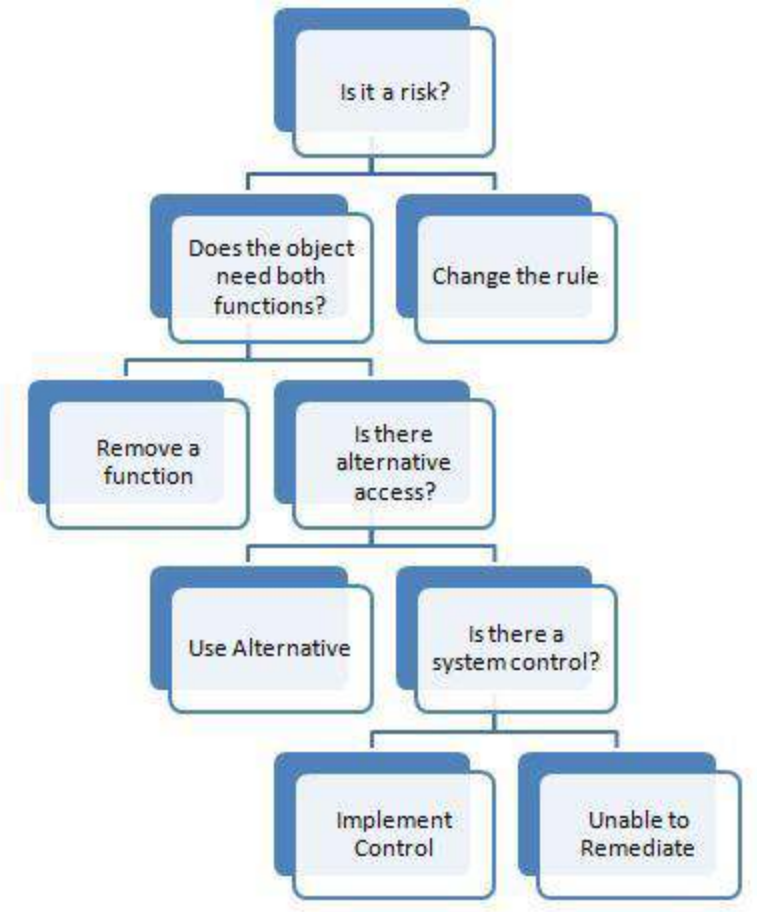
How can I decide remediation approach?

The diagram below has been devised to visually represent the process to deciding how to remediate the access. You may devise a similar approach and change the sequence of options depending on your organisation's policy.

Is it a Risk?: Before investing work effort into remediation you need to verify that violation is actually a risk and not a false positive.You may have executed the report at Action level only but if you re-ran at permission the violation is not longer there. Alternatively, you may look at the violation and question why it is a risk in the first place. If you realise the risk definition is incorrect then you need to change it. The rule-set (Business Risks / Rule Set) is not static and must be reviewed regularly.

Does the object need both functions?

The violation is a risk and you need to take action. Does the object (role, position, etc) require both actions? To assist in this decision you could look at action usage reports in GRC. If it appears one of the functions is not used, then remove it. For roles this will be a change request and users/positions it will be an Access Request. Approval from the business will be required regardless.



Is there Alternative Access?

You determined the both functions were used but could you assign a different transaction or authorisation combination to restrict. For example, the user might have XK01/02 transactions for Vendors but does not need all views – such as payments details. Instead they only need FK01/02 which does not include the payment details. By changing the transaction over the user can still perform their job function via a different transaction.

Is there a System Control – Can system controls via IMG configuration, workflow and ABAP development be implemented to remove the risk? Alternatively, can the business process be changed to include a new step. For example, add vendor confirmation via FK08/FL09 for sensitive fields to force a second pair of eyes to review the change.

Unable to Remediate – By this stage you have exhausted all possibilities to remediate the access and must investigate mitigation as an option.As already mentioned many times on SCN, always try to find a way to remediate a risk instead of defining compensating controls. Mitigation, whether it be with the help of spot checks, reviewing postings, etc. is always a reactive way and fraudulent actions might be done in the mean time. Still there needs to be a balance between managing risk and allowing the business to function. If you cannot remediate, refer to the document for further details on defining mitigating controls: Defining Mitigating Controls / Compensating Controls

Analyse Again (or verify your Remediation via Simulation)

Once you have remediated your risk we recommend you re-execute your risks analysis. You need to ensure that by remediating the list violations you did not introduce a new one. The good news with GRC is the ability to simulate access risk. Before going to the effort of role change or access change you can execute a risk simulation to test removing of the conflicting function and replacing with the alternative. This will provide you with confidence to remediate and avoid introduction of new risk. Using simulation will also reduce rework through continual rebuild or access change.

Finally I'm Finished – the system is clean…

Sorry to break it to you bust risk identification and analysis is continual. You must regularly plan to review your rule set to ensure the risks are valid (support packs, enhancement packs, custom development, changes to configuration, changes to the business, etc) as the system and business is in a constant state of change. In addition, when security role changes are migrated to production then user may now have risks.

Keep on top of the review so you only ever have a small number of violations to respond to. Scheduling Role Re-certification in BRM, SoD and UAR Review workflow will help manage this regular review.

Does your organisation approach remediation in GRC differently? We would love to hear your feedback in the comments below.

Best regards,

Alessandro Banzer & Colleen Hebbert

Alert Moderator

Assigned Tags

SAP Access Control | SAP Process Control | SAP Risk Management | Governance Risk And Compliance | governance risk and compliance sap grc | grc | grc 10

View more...

Similar Blog Posts

ARA - For the new kid on the block

By S A Aug 27, 2014

SAP Success Factors Employee Central and its integration with SAP GRC Risk Analysis & Access Request

By Ritika Mehrotra May 12, 2020

Mitigating controls - is this a cure for \"all evil\" in excessive authorizations risks in SAP? (part 1/5)

By Filip Nowak Dec 01, 2022

Related Questions

Seeking Best practice solution for remediating risks present in SOD Review requests :

By Sanjeev Kotwal Oct 15, 2019

Risk SO20: Function SD04 - Sales Document Release and Function SD05 – Sales Order Processing

By Rajashekar Chandrashekar Jun 18, 2017

Sensitive Access risk vs. Segregation of Duties violations risk reports

By Former Member Aug 08, 2017

26 Comments

You must be Logged on to comment or reply to a post.

Frank Koehntopp

August 25, 2014 at 12:49 pm

Hi Colleen & Alessandro,

great explanation of what remediation - on a technical level - means in Access Control.

The first thing to tell customers is (as you're mentioning, but it should be said in big, bold letters): this is NOT a project, it's about getting incrementally better by continually fixing stuff and discontinuing doing things wrong.

Mainly this means implementing two organisational controls; GRC ARA is nothing but a technical support tool to do that:

- no more changes to authorizations (roles, profiles) that are not going through ARA (Risk Terminator if you must). That should make sure that roles and profiles do not get worse from now on, in regard to SoD.

- no more authorization assignments that are not checked. Again, this ensures things do not get worse, and authorization administrators get used to being sensitive about access risk.

Those two controls do not need to be watertight and will allow many exceptions in the start, but they will create awareness and can be tuned over time.

Like 0 | Share

Prasant Kumar Paichha

August 25, 2014 at 2:05 pm

Hey...

good... but for the first time.. feel something uneasy with the picture or process flow.

perhaps, i should send you the one i have created for my projects.. that's been revised 12 times now.

Regarsd,

Prasant

Like 0 | Share

Colleen Hebbert

August 25, 2014 at 2:16 pm

Hi Prasant

Thank you for your feedback. The diagrams are more up at a conceptual level to show the aspects to consider. Ofcourse are ways to represent such content. What specially made you feel uneasy?

Always happy to take on board feedback and ways to improve content - especially if there is a way to improve quality content for this community. I am hesitant in accepting your offer based on what you have said. If you have produced your process flow for a project (and revised it 12 times) does that content (intellectual property) belong to your or your client? Ofcourse, if you own the IP then that is a different story 🙂

Regards

Colleen

Like 0 | Share

Prasant Kumar Paichha

August 25, 2014 at 2:22 pm

Revised 12 times means has been modified as er my clients requirement.

I have a standard document for remediation .

I have only confusion with the process flow, where risk is identified later.

Regards,

Prasant

Like 0 | Share

Colleen Hebbert

August 25, 2014 at 2:32 pm

Hi Prasant

I understood about your 12 refinements. However, you have produced this for a customer then we would need their permission to re-produce it and use is on SCN unless you hold rights to the content. I'm still unsure by your statement whether you own the material or not.

In terms of your confusion, which part. Risk is not identified later. The flow diagram assumes there is risk. Admittedly, I would have added the 'Yes' and 'No' labels for decision-flow but was trying to keep it simple. The 'Is it a Risk?' involves asking if the rule violation is actually a risk to the business. If not, there is a false positive and the rule set needs modifying. Otherwise, the rest of the flow diagram assumes there is risk to remediate (or mitigate)

Regards

Colleen

Like 0 | Share

Prasant Kumar Paichha

August 25, 2014 at 7:12 pm

Hello Colleen,

U have my document which is not for my client ,

so i do not need any permission from them .will post it here for references.

This i have created when i was new gradually improved with little experiences day by day.

Refards

Prasant

Like 0 | Share

Colleen Hebbert

August 25, 2014 at 9:35 pm

Thanks for your offer. I have followed you so can discuss in private outside of this post.

Like 0 | Share

Kanika Gupta

July 2, 2020 at 9:34 pm

Hi Prashant,

I am new to GRC area. Can you share that document with me?

Regards

Kanika

Like 0 | Share

Former Member

August 25, 2014 at 2:14 pm

Hi Alessandro,

Thanks for sharing this pictorial info in detail. Good to see your contents, like always.

For remediation process, with the screen shots from NWBC would be more useful and understandable to the audience. What do you say 🙂

Thanks,

Ameet

Like 0 | Share

Former Member

August 25, 2014 at 2:21 pm

This is a very good document; thank you for posting it. To me, the most important point is the last one: this is not just a "project" that is "complete." After the initial project, the effort needs to transition into an ongoing support process. It is very easy for the business to push back and claim that "our business processes never change" when they are not closely involved in testing the changes to the roles done with every support pack/ enhancement pack. If they were

more involved in the testing, with new transactions emphasized, the conclusion would follow naturally that the rule set must be maintained on an ongoing basis. Otherwise, you end up with a false sense of security in your "clean" system.

It is also important that mitigations actually mitigate the risk, whether they are preventive or detective. A "mitigation" that says nothing more than "these users are exempt from the rules" is not really a mitigation. Accepting a risk can be a legitimate strategy, but it is not the same as actually mitigating the risk. Fake mitigations give a false "clean" report, that will eventually come back to haunt the organization.

Cheers,

Gretchen

Like 0 | Share

Frank Koehntopp

August 25, 2014 at 2:29 pm

Excellent point on the mitigations - that's probably one of the most mis-used words in the GRC context.

I had one customer where one of the 'Big 4' consultancies had them upload a 20.000 line Excel file for their users with blanket 'mitigations' for all open issues - talk about false sense of security...

The other fallacy is resisting risk because 'the auditors never complained' - this needs to be an assessment _by_ and _for_ the company, not necessarily for the auditors. You don't want to be limited by what your auditors know or don't know about your organisation.

Like 0 | Share

Colleen Hebbert

August 25, 2014 at 3:47 pm

I hear this as the reaction all the time - to try to clear the number. Quite common the business wants to make exceptions for specific people - being who they are seems to make them more special or trust. I find myself biting through my tongue and commenting that the number of fraud cases out there are usually done by people in trusted positions and process was not followed!

> *Accepting a risk can be a legitimate strategy, but it is not the same as actually mitigating the risk.*

The goal of this blog was not to get to tied down in the theory of risk management (although a worth topic). However, we did try to cover off on that at a high level - remediate as a first option; followed by mitigation; followed by transfer or accept. Each option requires a cost benefit analysis. But yes, too often I am faced with people say 'we just accept it' but they have not considered what they are truly accepting and the cost of such a gamble. They then build a "control" to clear it.

Admittedly, I did recently recommend a 'defer-action' mitigating control that did not actually mitigate risk. However, the intended purpose was to allow them to assign a control for a few days to clear the SoD Access Review WF where they disagreed on the risk definition. This was due to separating who could create controls, approve and review access whilst at the same time review the rule set. I would have preferred embedding the ruleset prior to switching on SoD Review to avoid doing this. The 'defer-action' control was routing to specific approvers so they would be aware of the situation and investigate immediately. By the time a decision is made, the assignment should have expired to flag out the the unmitigated risk again (or rule set fixed and no longer flagging as a risk). Hopefully, second time round the 'defer-action' control is not selected.

But that solution was not on par with mass uploading permanent assignments of blanket assignment.

Regards

Colleen

Regards

Colleen

Like 0 | Share

Former Member

August 25, 2014 at 3:55 pm

Colleen,

At least "defer action" acknowledges that the risk is not yet remediated and needs future attention, and the expiry date is a good tool to enforce that follow up.

Gretchen

Like 0 | Share

Colleen Hebbert

August 25, 2014 at 4:03 pm

Exactly - and I only recommended it as the Approver was unable to submit the SoD WF Review without completing all items. It was devised to match the system but a process underpin it.

Like 0 | Share

Former Member

December 30, 2015 at 7:32 am

thanks for the idea with defer action, Colleen!

Like 0 | Share

Jean-Luc DENE

February 7, 2017 at 4:29 pm

Hello,
Please can you explain what "imparting" means here? Sorry I am French and English is my second language.
Many thanks in advance for your clarification.
Regards,
Jean-Luc

Like 0 | Share

Alessandro Banzer | Blog Post Author

March 23, 2017 at 7:57 pm

Dear Jean-Luc,

that means roles that are part of other roles. E.g. single roles that are part of several composite roles.

Cheers,

Alessandro

Like 0 | Share

Former Member
March 16, 2017 at 5:09 pm

Hi ,

Can anyone tell me how to find one single role which is assigned to how many composite roles in GRC NWBC.

Sunil

Like 0 | Share

Alessandro Banzer | Blog Post Author
March 23, 2017 at 7:54 pm

Hi Sunil,

did you check from Role Search / Role Maintenance in Additional Details > Where-used Roles?

Regards,

Alessandro

Like 0 | Share

Alessandro Banzer | Blog Post Author

March 23, 2017 at 7:56 pm

Also, there is a report available from Reports & Analytics. It's "Single to Composite Role Relationship".

Cheers,

Alessandro

Like 0 | Share

Former Member

May 29, 2017 at 3:58 pm

YES ,

Perfect .

Thank you Banzer.

Like 0 | Share

Former Member
May 29, 2017 at 4:01 pm

I have one more question .

Can any one tell me how many ways are there that we can create Mitigation controls in NWBC .

thanks in advance ,

Sunil

Like 0 | Share

Former Member
May 30, 2017 at 7:23 am

Hi suneel you may like This post

Creation of Mitigation Controls in GRC 10.0

Like 0 | Share

Former Member
May 31, 2017 at 4:50 pm

Thanks Nagesh above details.

Can we create Mitigation controls in via Process controls?

Thanks

Like 0 | Share

Former Member
July 30, 2017 at 11:44 am

Thanks a lot for your helpfull informations BR Hp

Like 1 | Share

Abdul Saleem
November 3, 2020 at 10:40 am

Rightly Explained!! There are plethora of challenges a business owner has to face out of which these are the common ones. Keep sharing your knowledge. here is an article that explains how digitization can aid your business.

Like 0 | Share

Find us on

Privacy	Terms of Use
Legal Disclosure	Copyright
Trademark	Cookie Preferences
Newsletter	Support